

Hot Topics in Privacy Enforcement: Key Trends in FTC, State, and Private Enforcement

Presented by

D. Reed Freeman, Jr.
Partner, ArentFox Schiff
Reed.Freeman@afslaw.com

Tracy Pulito
Global Chief Privacy Counsel
tracy.pulito@interpublic.com

Michelle R. Bowling
Associate, ArentFox Schiff
Michelle.Bowling@afslaw.com

Top Areas Of Risk in 2023 and Beyond

1. Consumer rights and business/controller obligations, including with respect to the Global Privacy Control;
2. Targeted advertising and profiling (so-called “commercial surveillance”);
3. “Dark patterns” in user interfaces and consumer choice mechanisms;
4. Children’s privacy and laws regulating design requirements for children;
5. Collection and use of biometric identifiers by employers and consumer-facing companies;
6. Display of videos and the use of social media pixels;
7. Use of online session replay scripts and online chat features; and
8. Collection and use of location data.

This year, we will see five U.S. state privacy laws take effect.

Effective January 1, 2023

- The California Privacy Rights Act (“CPRA”), which amends the California Consumer Privacy Act (“CCPA”)
- Virginia Consumer Data Protection Act (“CDPA”)

Effective July 1, 2023

- Colorado Privacy Act (“CPA”)
- Connecticut Act Concerning Personal Data Privacy and Online Monitoring (“CTDPA”)

Effective December 31, 2023

- Utah Consumer Privacy Act (“UCPA”)

U.S. State Laws: Recently Passed

Iowa, Indiana, Montana, and Tennessee all recently passed comprehensive state privacy legislation.

Iowa Consumer Data Protection Act (Senate File 262) – Effective January 1, 2025

- Business-friendly and similar to VCDPA and UCDPA.
- Provides 90-day right to cure (no sunset).
- No rulemaking or separate privacy enforcement agency; enforcement by state AG.

Indiana Consumer Data Protection Act – Effective January 1, 2026

- Business-friendly and similar to VCDPA and UCPA.
- 30-day cure provision with no sunset.
- Secondary use requires prior notice.
- No rulemaking or separate privacy enforcement agency, but plenty of time for amendments.

U.S. State Laws: Recently Passed and Awaiting Enactment

Montana Consumer Data Protection Act (Senate Bill 384) – Effective October 1, 2024

- Aligns most closely with Connecticut Data Privacy Act.
- Lowers applicability threshold of personal data processing to 50,000 or more MT residents.
- Provides 60-day right to cure, which sunsets April 1, 2026.
- Enhanced privacy requirements for sale or targeted advertising involving children 13-15.

Tennessee Information Protection Act – Effective July 1, 2025

- Aligns most closely with Virginia Consumer Data Protection Act.
- Requires adherence to NIST framework.
- Affirmative defense for controllers and processors who create, maintain, and comply with written privacy program.
- 60-day right to cure (no sunset).

U.S. State Laws: Recently Passed and Awaiting Enactment

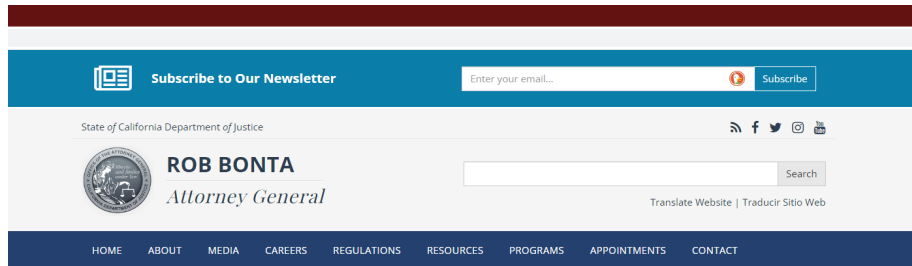
Washington's My Health My Data Act - Effective date March 31, 2024 (with 90-day delay for small business)

- Broad scope whose **purpose is to “supplement” HIPAA:**
 - “Consumer health data” is “personal information that is linked or reasonably linkable to a consumer and that identifies a consumer's past, present, or future physical or mental health.”
 - Applies to Washington residents **and individuals whose consumer health data is collected in WA.**
 - Regulated entities include any entity that: (1) conducts business in Washington or targets products or services to Washington consumers; and (2) determines the purpose and means of collecting, processing, sharing, or selling consumer health data.
- Requires opt-in consent before collecting or sharing consumer health data unless necessary to provide a product or service to the consumer.
- Requires “valid authorization” from consumer prior to sale, along with prescriptive notice requirements.
- **Private right of action available** under the Washington Consumer Protection Act.
- **Restrictions on placement of geofencing** around entities providing in-person healthcare if used to track consumers, collect their health data, or to send messages or ads relating to consumer health data or health care services. **This requirement goes into effect 90-days after passage.**

U.S. State Laws: Consumer Rights

- Right to access
- Right to confirm personal information processing
- Right to data portability
- Right to deletion
- Right to correction of inaccuracies/right of rectification
- Right to opt-out of “sale” of personal information
- Right to opt-out of targeted advertising/“sharing” for cross-contextual behavioral advertising

U.S. State Laws: Consumer Rights and Notable Differences



Ahead of Data Privacy Day, Attorney General Bonta Focuses on Mobile Applications' Compliance with the California Consumer Privacy Act

Press Release / Ahead of Data Privacy Day, Attorney General Bonta Focuses on...

Friday, January 27, 2023

Contact: (916) 210-6000, agpresso@doj.ca.gov

OAKLAND – Ahead of Data Privacy Day, California Attorney General Rob Bonta today announced an investigative sweep, sending letters to businesses with mobile apps that fail to comply with the California Consumer Privacy Act (CCPA). This year's sweep focuses on popular apps in the retail, travel, and food service industries that allegedly fail to comply with consumer opt-out requests or do not offer any mechanism for consumers who want to stop the sale of their data. The sweep also focuses on businesses that failed to process consumer requests submitted via an authorized agent, as required by the CCPA. Requests submitted by authorized agents include those sent by Permission Slip, a mobile application developed by Consumer Reports that allows consumers to send requests to opt-out and delete their personal information.

"In California, consumers have the right to stop the sale of their personal information, and my office is working tirelessly to make sure that businesses recognize and process consumers' opt-out requests," said Attorney General Bonta. "On this Data Privacy Day and every day, businesses must honor Californians' right to opt out and delete personal information, including when those requests are made through an

Right to Opt-Out of "Sale"

- **CA, CO, CT:** define a "sale" as an exchange for **monetary or other valuable consideration.**
- **VA and UT:** define a "sale" as an exchange for **monetary consideration only.**

U.S. State Laws: Consumer Rights and Notable Differences, Cont'd.

- **Right to object to/opt out of automated decision-making**
- **Right to object to or opt-out of profiling**
 - Of course you don't engage in profiling, right?
 - Not so fast!
 - **CA:** Any form of automated processing of personal information...to evaluate certain personal aspects relating to a natural person...and in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.
 - **CO, CT, VA:** Profiling must be in furtherance of decisions that produce legal or similarly significant effects (e.g., denial of loan or housing).

U.S. State Laws: Consumer Rights and Notable Differences, Cont'd.

- **Right to limit the use and/or disclosure of Sensitive Personal Information**
 - **CA** requires a “Limit the Use of My Sensitive Personal Information” link*
 - **Note:** Cookie banner is not an acceptable means of opt-out.
 - **VA, CO, and CT:** require **opt-in consent to process sensitive personal information.**
- **Right to non-discrimination**
 - Businesses/controllers cannot treat consumers differently based upon the exercise of consumer rights.

* CA allows the use of an alternative opt-out link, such as “Your Privacy Choices” in lieu of providing *both* a “Do Not Sell or Share My Personal Information” and the “Limit the Use of My Sensitive Personal Information” link.

U.S. State Laws: Business/Controller Obligations

Data protection assessments – **Be Careful, These Are Evidence!**

- Required by CA, CO, CT, VA

Generally required where:

- processing presents a significant risk to the individual's privacy or security
- processing of personal data for targeted advertising
- sale of personal data
- processing of personal data for profiling purposes, where there is a reasonably foreseeable risk to the individual
- processing of sensitive personal data
- processing presents heightened risk to the individual (e.g., unfair or deceptive treatment, financial or other injury, personal or physical intrusion)

U.S. State Laws Spotlight: Opt-Out Preference Signals

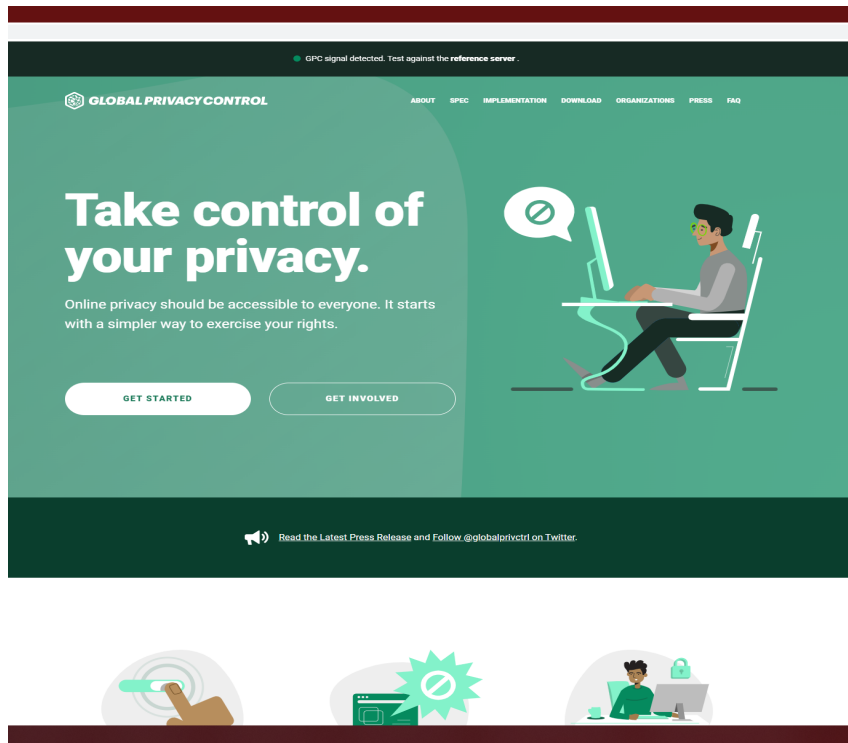
What is an “opt-out preference signal”?

- A signal sent by a platform, technology, or mechanism on behalf of the consumer that **communicates a consumer’s choice to opt-out of a sale or sharing of personal data.**
- Colorado refers to these as “universal opt-out mechanisms” (“UOOMs”).
- The California Attorney General has endorsed the Global Privacy Control as providing a valid opt-out preference signal.
- **Replace “Do Not Track”? Not Clear!**

Purpose:

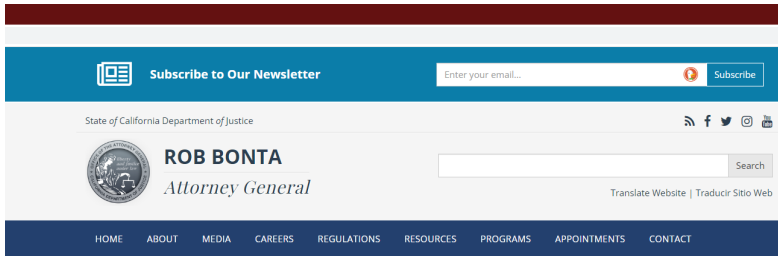
- **Provide consumers with a simple and easy-to-use method by which consumers interacting with businesses online can automatically exercise their right to opt-out of sale/sharing.**
- Through an opt-out preference signal, a consumer can opt-out of “sale” and “sharing” of their personal information with all businesses they interact with online **without having to make individualized requests** with each business.

U.S. State Laws Spotlight: Opt-Out Preference Signals, Cont'd.



- In effect in California now!
- As of **July 1, 2024, for Colorado** and **January 1, 2025, for Connecticut**, businesses (controllers) that process personal data for targeted advertising or sales must allow consumers to opt out via these signals.
- The Colorado Privacy Act's regulations contain prescriptive compliance requirements for honoring UOOMs.

U.S. State Laws Spotlight: Opt-Out Preference Signals, Cont'd.



Attorney General Bonta Announces Settlement with Sephora as Part of Ongoing Enforcement of California Consumer Privacy Act

Press Release / Attorney General Bonta Announces Settlement with Sephora as ...

Wednesday, August 24, 2022

Contact: (916) 210-6000, agpresso@doj.ca.gov

Marks strong second year of CCPA enforcement with update on enforcement efforts and new investigative sweep of businesses failing to process opt-out request via a user-enabled global privacy control

OAKLAND – California Attorney General Rob Bonta today announced a settlement with Sephora, Inc. (Sephora), resolving allegations that the company violated the California Consumer Privacy Act (CCPA), California's first-in-the-nation landmark privacy law. After conducting an enforcement sweep of online retailers, the Attorney General alleged that Sephora failed to disclose to consumers that it was selling their personal information, that it failed to process user requests to opt out of sale via user-enabled global privacy controls in violation of the CCPA, and that it did not cure these violations within the 30-day period currently allowed by the CCPA. Today's settlement is part of ongoing efforts by the Attorney General to enforce California's comprehensive consumer privacy law that allows consumers to tell businesses to stop selling their personal information to third parties, including those signaled by the Global Privacy Control (GPC).

Think you have time to comply? Not so fast...

The first CCPA enforcement action by the California Attorney General was against Sephora in August 2022.

Among the allegations was that Sephora failed to respond to opt-out preference signals as valid consumer opt-out requests.

Sephora settled for \$1.2 million.

European Economic Area

- February 2023 – Large social media company was fined €390 million by the Irish Data Protection Commission, which argued that the company **breached Article 6 of the GDPR** because “performance of a contract” could not be used as a legal basis for processing personal data for behavioral advertising where **platform users had to agree to data collection** for that purpose to use the services. Company is appealing the decision.

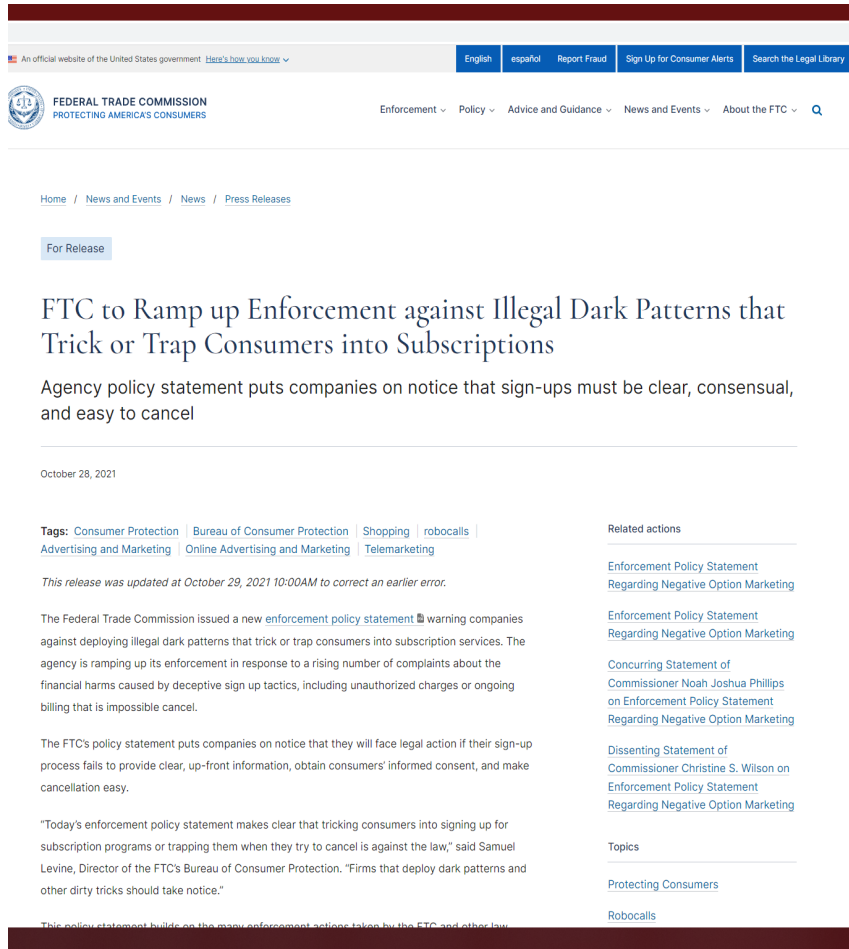
U.S. Enforcement Action

- California – In late January 2023, the California Attorney General released a statement that his office had completed an “investigative sweep” of popular mobile applications in retail, travel, and food service industries that resulted in businesses receiving letters regarding their noncompliance. One area identified was the **failure of businesses to process opt-out and data deletion requests**, especially those sent via privacy tools, such as the Global Privacy Control, or via authorized agents.

Targeted Advertising and Profiling: Key Takeaways

- ✓ Review legal basis for collection and processing of personal data for targeted advertising/profiling purposes.
- ✓ Ensure your business can honor data subject requests.

The CCPA/CPRA defines a dark pattern as, **“a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice.”**



The screenshot shows the FTC website's press release page for October 28, 2021. The main heading is "FTC to Ramp up Enforcement against Illegal Dark Patterns that Trick or Trap Consumers into Subscriptions". The sub-heading reads: "Agency policy statement puts companies on notice that sign-ups must be clear, consensual, and easy to cancel". The date "October 28, 2021" is displayed. The "Tags" section includes: Consumer Protection, Bureau of Consumer Protection, Shopping, robocalls, Advertising and Marketing, Online Advertising and Marketing, and Telemarketing. A note states: "This release was updated at October 29, 2021 10:00AM to correct an earlier error." The main text begins: "The Federal Trade Commission issued a new enforcement policy statement warning companies against deploying illegal dark patterns that trick or trap consumers into subscription services. The agency is ramping up its enforcement in response to a rising number of complaints about the financial harms caused by deceptive sign up tactics, including unauthorized charges or ongoing billing that is impossible to cancel." It continues: "The FTC's policy statement puts companies on notice that they will face legal action if their sign-up process fails to provide clear, up-front information, obtain consumers' informed consent, and make cancellation easy." A quote follows: "Today's enforcement policy statement makes clear that tricking consumers into signing up for subscription programs or trapping them when they try to cancel is against the law," said Samuel Levine, Director of the FTC's Bureau of Consumer Protection. "Firms that deploy dark patterns and other dirty tricks should take notice." A final line at the bottom reads: "This policy statement builds on the many enforcement actions taken by the FTC and other law."

- **Section 5 of the FTC Act prohibits “unfair or deceptive acts or practices in or affecting commerce.”** Using this authority, the FTC has brought hundreds of privacy and data security cases.
- In October 2021, the FTC released an enforcement policy statement on **“trick or trap” dark patterns**, which are methods used to induce consumers into signing up for subscription programs and then making it difficult for the consumer to cancel. This was followed by the FTC pursuing settlements against companies that renewed memberships without consent.

In September 2022, the **FTC issued a report** called ["Bringing Dark Patterns to Light"](#) in which it highlighted **four of the most common dark pattern tactics** employed by companies, including:

1. Difficulty in canceling subscriptions or charges

- The FTC has filed actions against companies that **required users to navigate multiple screens** in order to cancel subscriptions.

2. Misleading consumers and disguising advertisements

- Designing advertisements to look like independent editorial content. FTC states that even adding disclaimers to fake editorial content are **unlikely to overcome a "deceptive net impression."**
- ***Effen Ads – December 2019.*** Operators of a work-from-home scheme sent unsolicited emails to consumers that included "from" lines that falsely claimed they were coming from CNN or Fox News and also routed to fake online news stories that eventually routed to Effen Ads' sales websites. Operators agreed to a **\$1.5 million settlement.**
- **Also includes countdown timers or indicators that the supply is almost sold out to induce action.**

Dark Patterns: FTC Enforcement, Cont'd. & Class Actions

3. Hiding key terms and “junk fees”: *Vonage* – November 22

- The FTC alleged that Vonage, an internet phone service provider, **subjected its customers to dark patterns and junk fees** when trying to cancel the services. Vonage was required to revise its T&Cs and simplify the cancellation process.
- Includes “**drip pricing**” in which companies advertise only part of a product’s total price to lure in consumers, and don’t mention mandatory charges until very late in the buying process. (Lending Club)

4. Tricking consumers into sharing unnecessary data

- This tactic, which is also the **highest enforcement priority** for the FTC, employs dark patterns which appear to provide consumers with a choice but intentionally steer them towards an option that provides the most personal information.

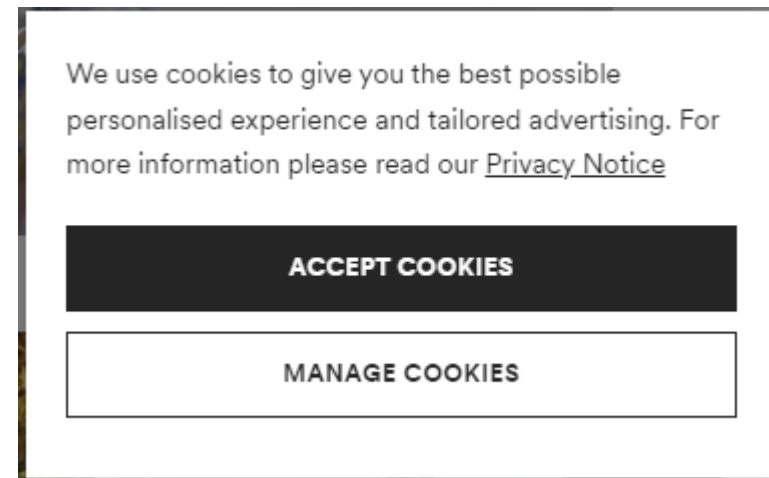
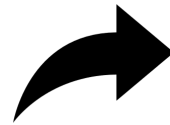
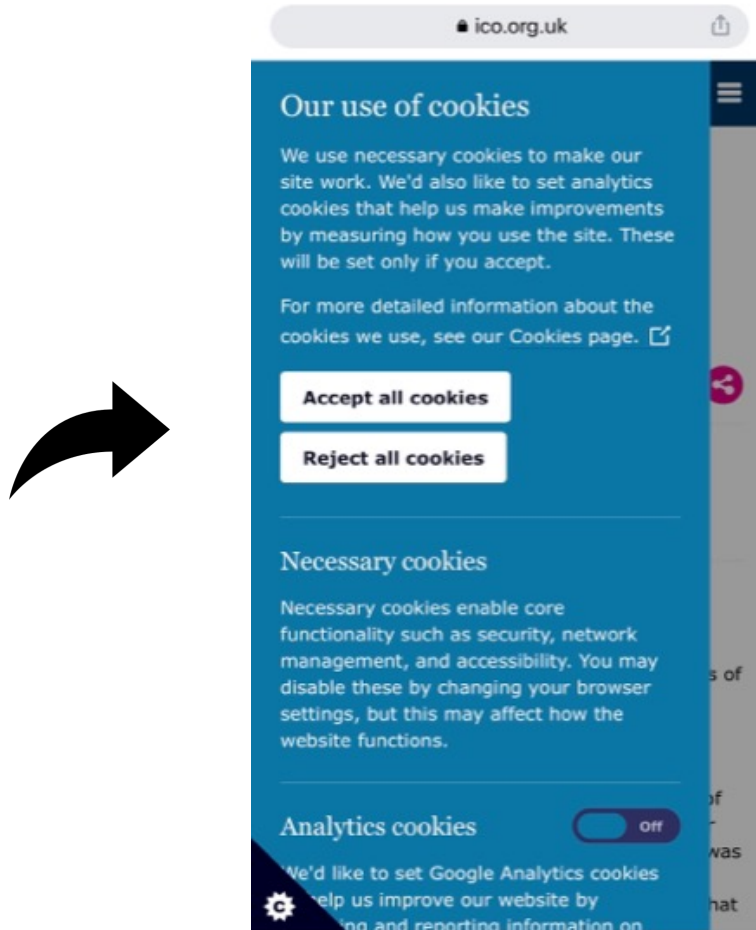
Class actions:

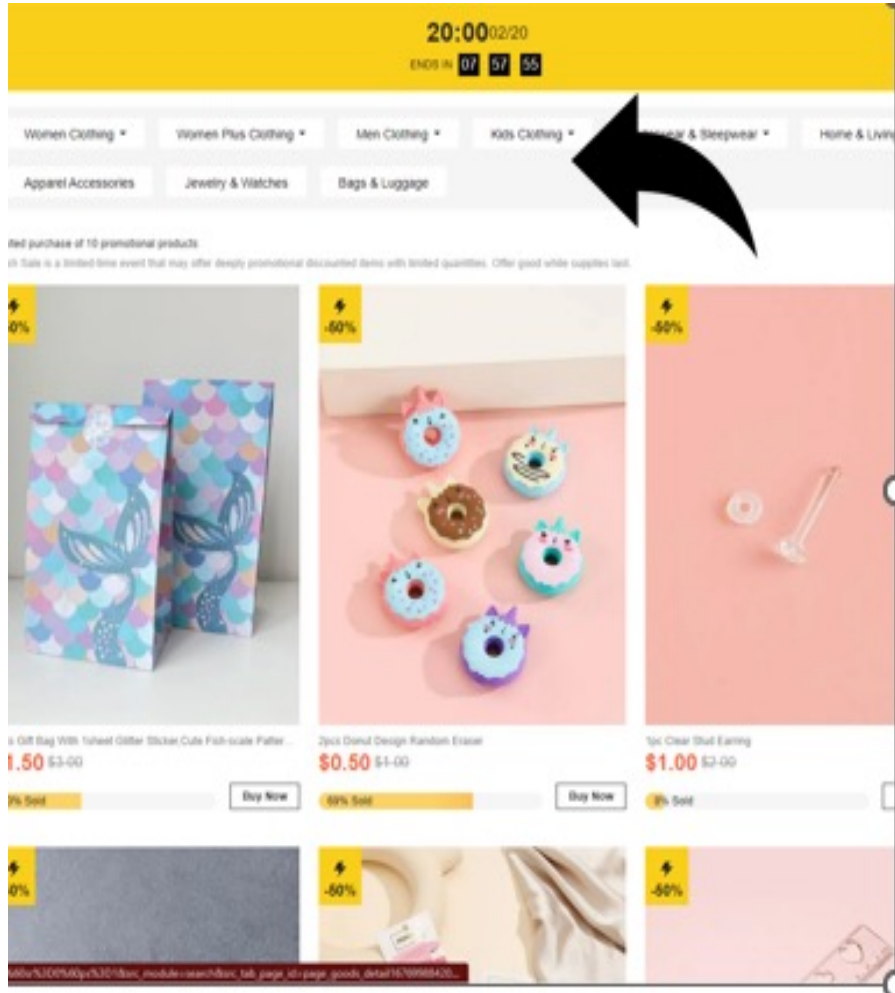
- Noom, which provides a weight loss app, settled a consumer fraud class action in New York for **\$62 million** in which it was alleged that Noom misled customers into signing up for low-cost trial subscriptions that led to expensive, difficult to cancel subscriptions. A former senior software engineer for Noom admitted that **cancelling was “difficult by design,”** a tactic used to generate revenue from consumers that failed to cancel in time to avoid charges.

Dark Patterns: U.S. State Regulation

California and Colorado have led the way, outlining methods for submitting consumer rights requests and obtaining consumer consent, which must meet the following requirements or risk being considered a dark pattern:

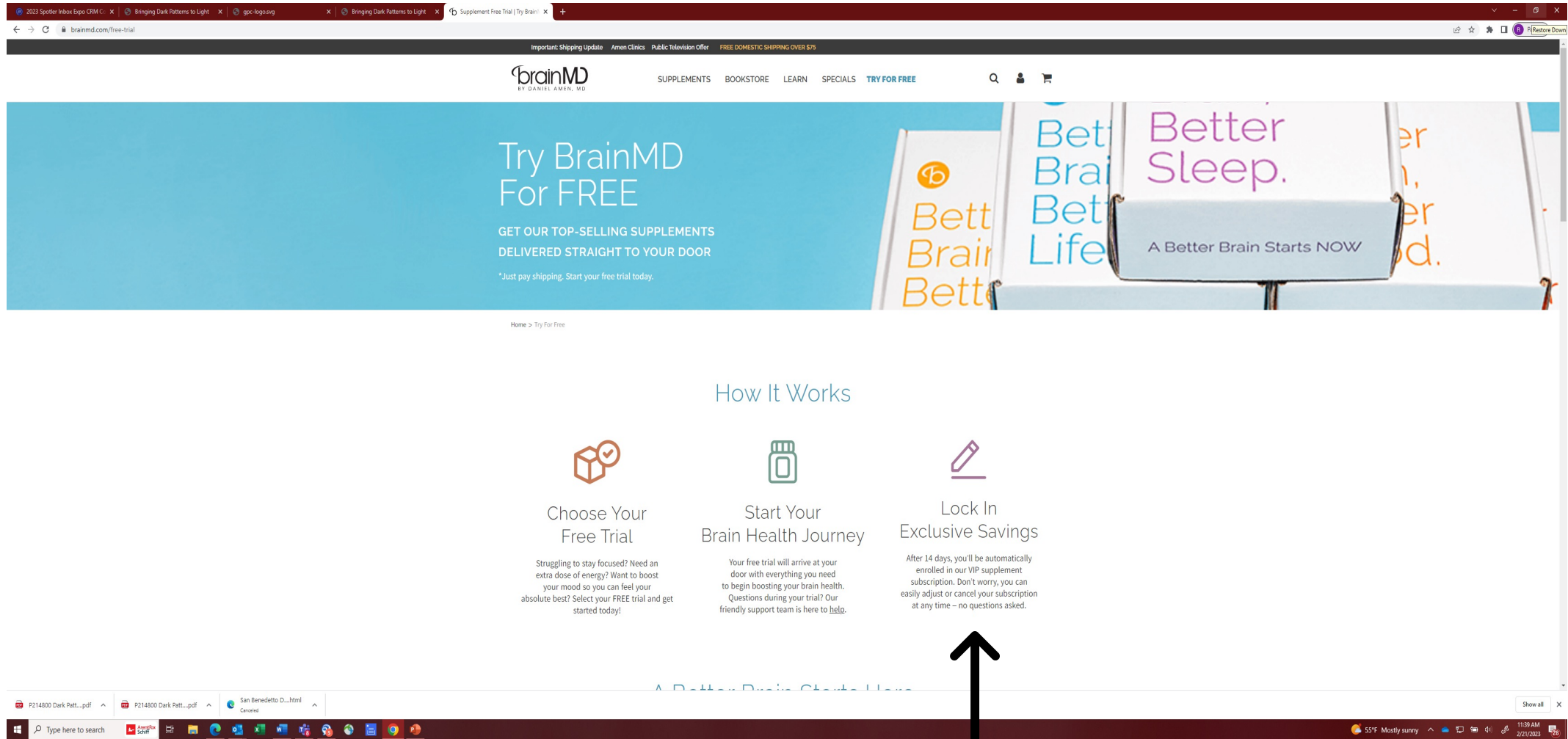
- **Easy to understand**
- **Symmetry of choice**
 - **Example 1:** Choice to opt-in to sale of personal information. Choices “Yes” and “Ask Me Later” are not symmetrical. “Yes” and “No” are symmetrical.
 - **Example 2:** Website cookie banner provides choices when seeking consent. “Accept All” and “More Choices” are not symmetrical. “Accept All” and “Decline All” are symmetrical.
- **Avoid language that is confusing to the consumer.**
 - **Example:** Double negatives such as choice of “Yes” or “No” next to “Do Not Sell or Share My Personal Information.”





Dark Patterns: Examples





Important: Shipping Update Amen Clinics Public Television Offer FREE DOMESTIC SHIPPING OVER \$75

brainMD
BY DANIEL AMEN, MD

SUPPLEMENTS BOOKSTORE LEARN SPECIALS TRY FOR FREE

Try BrainMD For FREE

GET OUR TOP-SELLING SUPPLEMENTS DELIVERED STRAIGHT TO YOUR DOOR

*Just pay shipping. Start your free trial today.

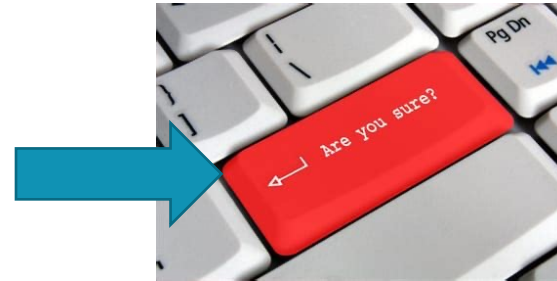
Home > Try For Free

How It Works

- Choose Your Free Trial**
Struggling to stay focused? Need an extra dose of energy? Want to boost your mood so you can feel your absolute best? Select your FREE trial and get started today!
- Start Your Brain Health Journey**
Your free trial will arrive at your door with everything you need to begin boosting your brain health. Questions during your trial? Our friendly support team is here to help.
- Lock In Exclusive Savings**
After 14 days, you'll be automatically enrolled in our VIP supplement subscription. Don't worry, you can easily adjust or cancel your subscription at any time – no questions asked.

A Better Brain Starts Now

- **Avoid choice architecture that impairs or interferes with the consumer's ability to make a choice.**
- **Examples of what to avoid:**
 - Requiring consumers to click through multiple screens.
 - Bundling choices for permitted business purposes with incompatible purposes.
- **Easy to execute.**
 - Clicking "Do Not Sell or Share My Personal Information" should take consumers to the mechanism to exercise rights and must not require a consumer to scroll through the entire policy.
- **Standard-Forcing** – The Colorado Privacy Act Rule 7.09(E)
 - "The fact that a design or practice is commonly used is not, alone, enough to demonstrate that any particular design or practice is not a Dark Pattern."



Dark Patterns: Key Takeaways

- ✓ Review methods of consent and choice architecture against FTC and state guidelines.
- ✓ Choice buttons should be the same size and color.
- ✓ Pay attention to consumer complaints, as these will often initiate investigations or enforcement actions. If possible, conduct consumer testing (e.g., FTC Epic Games Case).
- ✓ Avoid product or service “rankings” that give the impression of objective or unbiased reviews, especially where rankings are based on third-party compensation.
- ✓ Watch out for a false sense of urgency.
- ✓ Disclose any unavoidable, mandatory fees in the upfront, advertised price.

Children's Privacy

- President Biden, in his last two State of the Union addresses, urged Congress to take action.
- **FTC: Protection of children's data is an enforcement priority.**
 - Websites and other online properties that offer children's content are under increased scrutiny.
- **All comprehensive U.S. state privacy laws provide enhanced protections for children.**
- Utah signed into law two bills restricting social media's treatment of children, one of which prohibits the use of "addictive design features."
- Several other states have pending legislation that would require digital service providers to prevent harm to children (TX and LA) and would regulate social media's interaction with children (FL, LA, NC, and NY).

- **The Children's Online Privacy Protection Rule ("COPPA") regulates how websites, apps, and other online operators collect data and personal information from children under 13.**
- **Enforced by the FTC**
- **Key requirements** for operators of commercial websites and online services "directed to children":
 - Online privacy notice
 - Direct notice to parents
 - **Must obtain verifiable parental consent**
 - Data minimization
 - Provide parental access
 - Set data retention limits
 - Reasonable security

California's Age-Appropriate Design Code Act ("ADCA") – **effective July 1, 2024**

- Unlike COPPA, the ADCA has a much lower threshold of applicability, applying broadly to online services, products or features **likely to be accessed by children** whereas COPPA applies to online services, products or features, that are either directed to children, or in the case of general use products and services, that the operator has actual knowledge that they are being used by children.
- Also prohibits collecting, selling, or retaining a child's geolocation information; profiling by default; and leading or encouraging children to provide personal information.
- **Requires privacy disclosures** in terms of service, policies, and community standards to be easily accessible and enforced.
- **Data Protection Impact Assessments required** before offering new online services, products, or features likely to be accessed by children.
- COPPA, child is a person under 13. ADCA: CHILD IS 18.
- Minnesota and Nevada are considering similar legislation.

Children's Privacy: Recent Enforcement & Litigation

COPPA: ***Weight Watchers/Kurbo*** – March 2022: FTC alleged

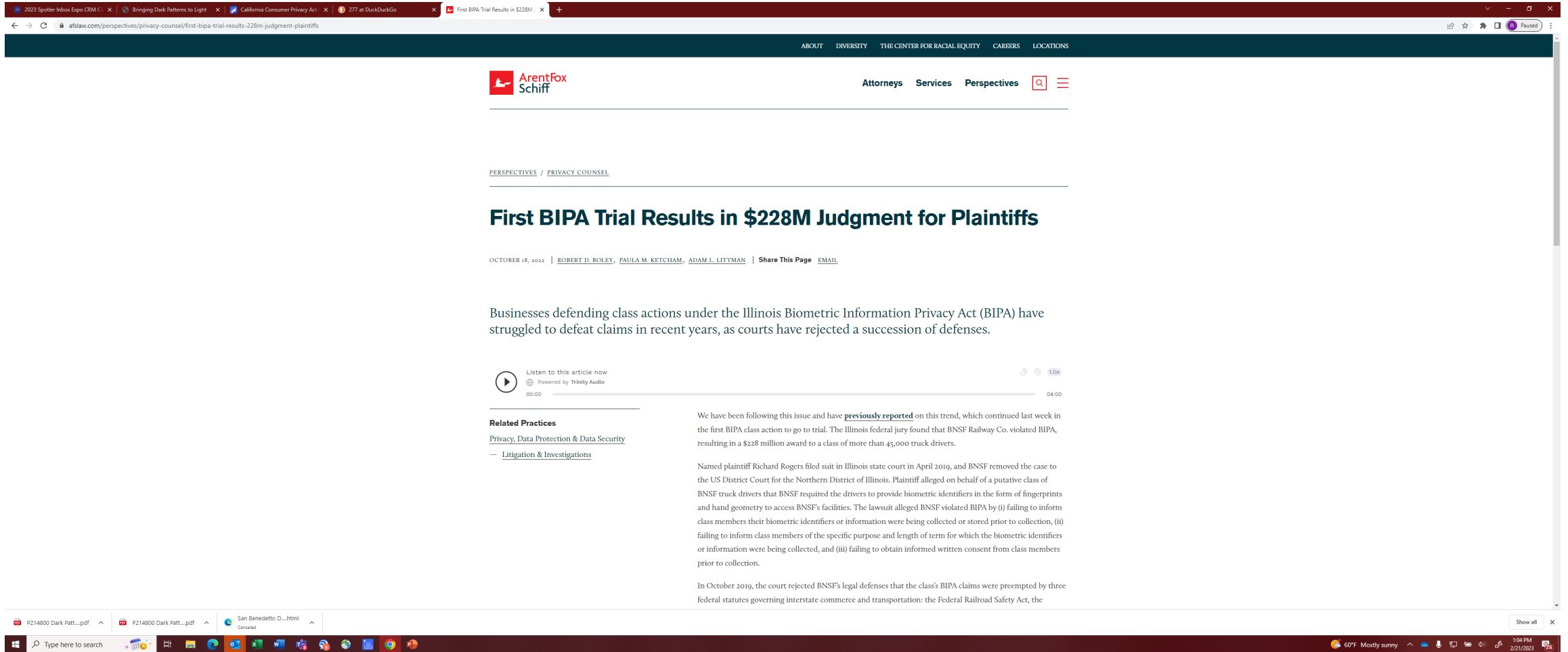
- Company **marketed a weight loss app for use by children** as young as eight and then **collected their personal information without parental consent**.
- Order: **\$1.5 million judgment**, required the company to **delete data it had allegedly illegally collected**, and also to **delete any models or algorithms developed** in whole or in part using personal information collected from children through the app. **Aka, "algorithmic disgorgement."**

COPPA: ***Epic Games, Inc.*** – December 2022. **More than Half a Billion Dollars!**

- FTC alleged that the creator of the video game "Fortnite," **violated COPPA by employing dark patterns** to trick millions of players into making unintentional purchases.
- **Epic will pay \$275 million penalty for COPPA violations** – the **largest penalty ever obtained** for violating an FTC rule – and also pay **\$245 million in refunds** to affected users. Epic was also ordered to change default privacy settings.

Children's Privacy: Key Takeaways

- ✓ Evaluate whether your website or application has children's content, regardless of whether it is "directed to" children.
- ✓ Collect verifiable parental or legal guardian consent.
- ✓ Honor opt-out and deletion requests.
- ✓ Treat children's data as sensitive personal information.
- ✓ Consider implementing an age-gate.
 - Note that a check box, such as "I am over 13," was deemed ineffective by the FTC in *Weight Watchers/Kurbo*.
 - Best practice is to use birthdate with month, date, and year.



2023 Spotler Inbox Expo CRM C... Bringing Dark Patterns to Light California Consumer Privacy Act 277 at DuckDuckGo First BIPA Trial Results in \$228M

afslaw.com/perspectives/privacy-counsel/first-bipa-trial-results-228m-judgment-plaintiffs

ABOUT DIVERSITY THE CENTER FOR RACIAL EQUITY CAREERS LOCATIONS

ArentFox Schiff Attorneys Services Perspectives

PERSPECTIVES / PRIVACY COUNSEL

First BIPA Trial Results in \$228M Judgment for Plaintiffs

OCTOBER 18, 2022 | ROBERT D. BOLEY, PAULA M. KETCHAM, ADAM L. LITTMAN | [Share This Page](#) [EMAIL](#)

Businesses defending class actions under the Illinois Biometric Information Privacy Act (BIPA) have struggled to defeat claims in recent years, as courts have rejected a succession of defenses.

Listen to this article now
Powered by Trinity Audio
00:00 04:00

Related Practices

- [Privacy, Data Protection & Data Security](#)
- [Litigation & Investigations](#)

We have been following this issue and have **previously reported** on this trend, which continued last week in the first BIPA class action to go to trial. The Illinois federal jury found that BNSF Railway Co. violated BIPA, resulting in a \$228 million award to a class of more than 45,000 truck drivers.

Named plaintiff Richard Rogers filed suit in Illinois state court in April 2019, and BNSF removed the case to the US District Court for the Northern District of Illinois. Plaintiff alleged on behalf of a putative class of BNSF truck drivers that BNSF required the drivers to provide biometric identifiers in the form of fingerprints and hand geometry to access BNSF's facilities. The lawsuit alleged BNSF violated BIPA by (i) failing to inform class members their biometric identifiers or information were being collected or stored prior to collection, (ii) failing to inform class members of the specific purpose and length of term for which the biometric identifiers or information were being collected, and (iii) failing to obtain informed written consent from class members prior to collection.

In October 2019, the court rejected BNSF's legal defenses that the class's BIPA claims were preempted by three federal statutes governing interstate commerce and transportation: the Federal Railroad Safety Act, the

P214800 Dark Patt...pdf P214800 Dark Patt...pdf San Benedetto D...html Canceled

Type here to search 60°F Mostly sunny 1:04 PM 2/21/2023

- Biometric data is an **increased focus of regulation** via new state privacy laws and also **a source of increased litigation**, especially in Illinois.
- Biometric data is regulated via Section 5 of the FTC Act, state privacy laws, biometric privacy laws, and in general or sector-specific laws (such as employment laws).
- Definitions vary, but biometrics generally refers to human biological measurements and behavioral characteristics, such as facial geometry, iris scans, and voiceprints when that data is used to identify or authenticate an individual.

- **Three states have specific biometric privacy laws, and currently, there is active legislation in at least nine additional states.**
 - Illinois Biometric Privacy Act (“BIPA”)
 - Texas Capture or Use of Biometric Identifier Act (“CUBI”)
 - Washington Biometric Law
- **BIPA provides for \$1,000 in statutory damages for each negligent violation and \$5,000 for each reckless or intentional violation.**
- State privacy laws: **CA, CO, CT, VA, and UT all consider biometric information** processed for uniquely identifying an individual **sensitive personal information.**

Maine

- Reintroduced a law similar to Illinois' BIPA and would be effective January 1, 2025.
- Requires written consent prior to the collection, selling, or retaining of an individual's, "voiceprint or imagery of the iris, retina, fingerprint, face or hand, that can be used to identify that individual."
- Includes a private right of action.
- Penalties per violation include \$1,000.00 for negligent violations, and \$5,000.00 for reckless or intentional violations.

New York City

- Lawmakers have introduced two bills to regulate private-sector use of biometric tech.
- One bill regulates the use of facial recognition or surveillance technology in private businesses - from stadiums to grocery stores - to identify customers, and any collection of face scans or fingerprints would require prior written consent from the customer.
- The other limits the installation and use of any biometric recognition technology in residential buildings to identify tenants or their guests. Both laws would take effect 180 days after being signed into law.

Biometric Privacy: Enforcement & Litigation

○ *Everalbum, Inc. – January 2021.*

- A California-based developer of a **photo storage app** settled with the FTC over allegations that it deceived consumers regarding its use of facial recognition technology, which was **enabled by default for most users** and without a way to disable the feature.
- As part of its settlement order, Everalbum had to delete not only the photos and videos of users who deactivated their accounts, but all models and algorithms developed using the photos and videos uploaded by its users – also known as “**algorithmic disgorgement**.” FTC develops its own common law through settlement order.

○ *Cothron v. White Castle – February 2023.*

- White Castle had **obtained employee’s fingerprints**, stored them in a company database, and then required workers to use their fingerprints to access paystubs or company computers.
- The Illinois Supreme Court ruled that **BIPA claims accrue each time data is unlawfully collected and disclosed** rather than the first time. **Defendant argued exposure could exceed \$17 Billion!**

Biometric Privacy: Enforcement & Litigation, Cont'd.

○ *Tims Class Action– February 2023*

- Tims filed a class action lawsuit against his former employer, alleging violations of BIPA, presenting a question of whether a one-year or five-year statute of limitations applies where BIPA is silent.
- Illinois Supreme Court ruled that a **five-year statute of limitations applies to all causes of action alleging violations under BIPA!!**

○ *Rodriguez Perez Class Action – filed March 16, 2023*

- Putative class action was filed by a Brooklyn, NY resident under **New York City's Biometric Identifier Information Law**, alleging that Defendant's grocery stores **collected data on customers' body size and shape** as part of the checkout process without providing notice as required under the law.
- Rodriguez Perez alleges that Defendant did not post signage about this biometric data collection until months after the law took effect in January 2022.

Biometric Privacy: Enforcement & Litigation, Cont'd.

BIPA Virtual Try-On cases:

- *Kukovec v. Estée Lauder Companies, Inc. – Nov. 2022.*
 - Allegation: Make-up try on tool deployed across websites owned by The Estée Lauder Companies allowed online users to upload a photograph or use the device camera to simulate product application. Litigation is pending on the allegation that Estée Lauder **negligently violated BIPA's notice and consent provisions.**
- *Theriot v. Louis Vuitton – Dec. 2022.*
 - Plaintiffs allege non-compliance with BIPA's notice and consent requirements via the third-party operator, FittingBox, which collects and processes facial geometry for an eyeglasses virtual try-on tool.
 - Court rejected Louis Vuitton's argument that FittingBox (which was not party to the litigation), collected and processed the biometric data rather than Louis Vuitton, finding that **Louis Vuitton collected the facial scans when it actively invited users to take advantage of the tool.**

Biometric Privacy: Key Takeaways

- ✓ Comply with notice, consent, and disclosure requirements.
- ✓ If acting as a service provider or third party, ensure that the business or controller is compliant with relevant laws to avoid getting pulled into litigation.
- ✓ Establish a written, publicly-available data retention and destruction schedule for biometric data.
- ✓ Implement security measures to protect biometric data.

Video Privacy Protection Act (“VPPA”) 1988

- Imposes liability on companies “engaged in the business ... of rental, sale, or delivery of prerecorded video[s]” **when they knowingly disclose personally identifiable information related to a consumer and their video viewing history.**
- Law is now being **used against general-purpose websites that contain video content**, alleging that a disclosure of video viewing history occurs **when tracking pixels communicate with third parties.**
- **Consumers are pursuing lawsuits against companies across industries**, from news outlets, sports organizations, to consumer products companies.

Display of Videos and the Use of Social Media Pixels: Key Takeaways

- ✓ Businesses using “plug and play” tracking technology and advertising software should **evaluate potential obligations under the VPPA.**
- ✓ **Obtain user consent prior to collection and disclosure** of personal information, especially sensitive personal information.

Session Replay Scripts and Online Chat Features

Another litigation trend involves an increase in lawsuits filed **alleging violation of state wiretapping laws** against companies employing session replay technology and chatbots. Wiretapping litigation is **currently most active in California, Florida, Illinois, and Pennsylvania.**

- **Session Replay Technology:** This technology allows a company to “replay” visits to its website to understand a user’s interaction with the website, such as what was viewed, clicked on, or hovered over.
- ***Popa v. Harriett Carter.*** Plaintiffs claimed unlawful surveillance in violation of Pennsylvania’s Wiretapping and Electronic Surveillance Control Act after shopping on Harriet Carter’s website, which used session replay technology.
- ***TikTok.*** On January 13, 2023, a putative class action was filed against TikTok in the Northern District of Illinois alleging that the social media platform tracked user activity on third-party websites in **violation of the Federal Wiretap Act.**

Session Replay Scripts and Online Chat Features

- **Chatbot Cases:** Plaintiffs, **primarily in California and now Florida**, allege that a website's use of digital tools to have automated "conversations" with site visitors, without first obtaining explicit consent, are a violation of state wiretapping laws.
 - In *Saleh v. Nike, Inc. (2021)*, the court found that where a third-party software has simultaneous, real-time access to a customer's website communications **without customer consent, the third-party vendor became a "wiretapper" and the website which allowed the wiretapping had "aided and abetted" the violation.**

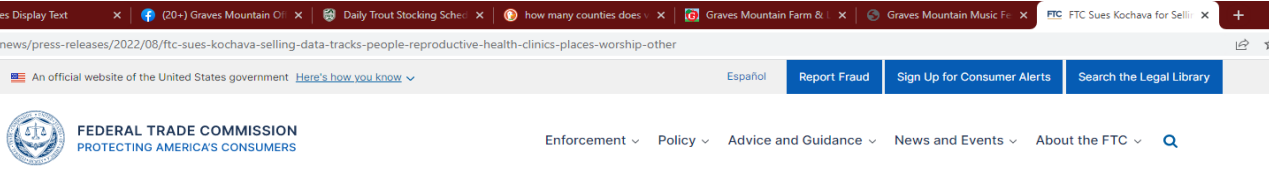
Session Replay Scripts and Online Chat Features: Key Takeaways

To be safe...

- ✓ **Provide notice and obtain affirmative consent** for the use of chatbots or session replay technology prior to collecting or processing any information, ideally **through a “just-in-time” consent pop-up.**
- ✓ **Privacy policies should be clear and transparent** in disclosing what technologies are used on the site and be conspicuous and accessible.
- ✓ **Beware the use of chatbots in states with all-party consent wiretapping laws.** These states include (broadly interpreted): California, Colorado, Connecticut, Delaware, Florida, Illinois, Maryland, Massachusetts, Montana, Nevada, New Hampshire, Oregon, Pennsylvania, and Washington.

Location data is often broken down into two categories: “coarse geolocation data” and “precise geolocation data”.

- **“Coarse geolocation data”**: Information that describes location with **less precision than a zip code**, such as the use of an IP address.
- **“Precise geolocation data”**: All 5 states with new privacy laws consider “precise geolocation data” to be sensitive personal information, either explicitly within the definition of SPI (CA, CT, VA, UT) or implied in its rulemaking (Colorado).
 - California defines “precise geolocation information” as any data that is **derived from a device** and that is used or intended to be used to locate a consumer within a geographic area that is equal to or less than the area of a circle with a radius of 1,850 feet.
 - Connecticut, Virginia, and Utah use a similar definition, but lower the threshold to 1,750 feet.
 - Colorado mentions “precise geolocation data” but does not provide a specific definition.
 - **VA, CO, and CT**: require opt-in consent to process sensitive personal information.



Home / News and Events / News / Press Releases

For Release

FTC Sues Kochava for Selling Data that Tracks People at Reproductive Health Clinics, Places of Worship, and Other Sensitive Locations

Agency Alleges that Kochava's Geolocation Data from Hundreds of Millions of Mobile Devices Can Be Used to Identify People and Trace Their Movements

August 29, 2022

Tags: [Consumer Protection](#) | [Bureau of Consumer Protection](#) | [Privacy and Security](#) | [Consumer Privacy](#) | [Health Privacy](#)

The Federal Trade Commission filed a lawsuit against data broker Kochava Inc. for selling geolocation data from hundreds of millions of mobile devices that can be used to trace the movements of individuals to and from sensitive locations. Kochava's data can reveal people's visits to reproductive

Related Cases

[FTC v Kochava, Inc.](#)

For Consumers

Since FTC sued Kochava that sells

Kochava, Inc. – August 2022: The FTC alleged that Kochava, a data broker, **sold geolocation data from millions of mobile devices** that **allegedly could reveal visits to sensitive locations**, including places of worship, addiction recovery facilities, and domestic violence shelters. The lawsuit is currently active.

Geolocation Data: Key Takeaways

- ✓ Evaluate the collection and use of geolocation information.
- ✓ Avoid collection and processing of precise geolocation information.
- ✓ If collecting precise geolocation information, confirm that you are obtaining consent where required or that you can honor opt-out requests.

Thank You!

Questions & Contact Information

Reed Freeman

Reed.Freeman@afslaw.com

Tracy Pulito

tracy.pulito@interpublic.com

Michelle Bowling

Michelle.Bowling@afslaw.com